بسم الله الرحمن الرحيم

السلام عليكم ورحمة الله وبركـاًته

سأتحدث اليوم عن طريقة أختراق الاجهزه الشخصيه بواسطة برامج الأختراق .. وكيف تتم هذه العمليه ..

أخاطب في هذا الدرس ، الجيل النـاشىء ، والمبتدئين ، وليس المحترفين .

أستحلفك بالله العظيم أن لا تستخدم أياً من المعلومات أدناه في إلحاق أي ضرر بأخوانك المسلمين .

تم نشر المعلومات لتعم الفائده ،

Here's a Hint :

Think Like a Hacker and avoid being HACKED !

Author :

Mohammed Nasser Al-Mawri

فهرس :

1– مقدمــه

لاشك أن الأغلب .. يعرف ماهي انظمة التشغيل ويعلم ايضاً أنهُ يمكن تركيب برامج على انظمة التشغيل تلك .. مهما كان نوعها [البرامج] .. فـ من برامج المحادثات ، والتواصل . مروراً بـ برامج الملتميديا وبرامج الاوفس وبرامج سطح المكتب .. الى البرامج الاضافيه وبرامج تنسيق سطح المكتب .. الخ

لكن هناك نوع آخر من البرامج .. وهذه البرامج ، تمثل صمام الأمان بالنسبه للمخترقين او الـ Hacker'z .. بالأصح kids .. وتلك البرامج هيَ .. برامج الأختراق والباتشات الناتجه عنها . او ما يسمى بـ تروجان / Trojan .. او أحصنة طرواده .. أو الأبواب الخلفيه / back door

كل هذه التسميات هي لنفس البرنامج .. ولا اقصد هنا برنامج الاختراق .. بل [البرنامج المصغر] الناتج عن برنامج الاختراق .. وهو مايطلق عليه الهكرز أسم patch / باتش ..

وهذه البرامج اذا تم تركيبها على نظام تشغيلك بأي طريقة كانت سواءً بـ إرادتك ام بغير ارادتك ..فهي تمكن المخترق من التحكم الكامل في جهازك . لا ينقصه الا ان يلمسه !

2- برامج الأختراق .

تختلف برامج الاختراق ، بناءً على سرعة نقل البيانات من جهاز الضحيه الى جهاز المخترق ، وايضاً على اساس استخدام البورت الذي يتم بواسطته نقل البيانات .. بين الطرفين [الهكر ، والضحيه] ..

وأغلب البرامج المتواجده حالياً .. والتي يتم استخدامها هي : bifrost , spy-net , trukjan , pison .. Etc

يوجد الكثيير من برامج الأختراق .. وكلها ، بُنيت على نفس الفكره .. وهي الـ client –to-server

ومن لا يعرف هذه الفكره !

مثال :

مقاهي الأنترنت .. تستخدم هذه الفكره في عدة برامج مثل [الحوباني سوفت ، Esay-café، Dway] وغيرها من برامج اداره المقاهي .. المعروفه لدى الجميع ..

تخيل أن المخترق هو [المحاسب / server] .. وأنت [زبون / client] ..

أولاً ، لا تستطيع استخدام الجهاز الا بأذن من الـ server .. ويستطيع السيرفر مراقبتك ، انشاء ملفات على جهازك .. الخ .. وكل ذالك يتم توفيره للـ[محاسب] .. بواسطة الخصائص التي يتحيها لهُ برنامج إدارة المقهى ..

وكذلك المخترق .. سيتمكن من التلاعب بجهازك كيفما شاء ، وفقاً للخصائص التي يوفرها لهُ برنامج الأختراق ..

Get it !

هذهِ هي فكرة برامج الأختراق ..

3 - باتش برنامج الأختراق / والمعلومات المخزنه عليه .

حسناً ! .. دعونا نوضح نقطه مهمه ، هنا في البدايه .. وهي عناوين أجهزة الحاسوب على الشبكة العنكبوتيه .. ويتكفل بهذا بروتوكل Tcp/ip .. وهوَ بروتوكل نقل الملفات وإستقبالها ، وايضاً هو البروتوكل المتكفل بوضع ip address خاص بجهازك .. وآي جهاز آخر يستخدم الأنترنت .. ويتم تغيير هذا الرقم الخاص بجهازك ، عندما تقوم بقطع اتصالك بالمودم .. والعوده مره أخرى .. يتم منحك ip address مختلف عن السابق ..

سؤال / يتبادر إلى الذهن !؟

-كيف يستطيع المخترق ان يتحكم في جهازي .. وقد قمت بتغيير رقم الـ ip address الخاص بي ؟ على أعتبار ان المخترق لا يستطيع اختراقي الا عن طريق معرفته للـ ip address الخاص بي ؟!

حسناً .. هنالك ما يسمى بالإتصال العكسيَ ..

ولكن ، في قبل التعمق .. دعوني اوضح لكم ماهية الباتش ، وكيف يعمل ..

.. عند قيام الهكر بإستخدام برنامج الهكر bifrost مثلاً .. يقوم أولاً بأنشاء [البرنامج المصغر / الباتش / Trojan / حصان طروآده] .. ويضع فيه الـ ip address الخاص بالمخترق / وليس الخاص بَك .. لأن الباتش يعمل فقط على أرسال البيانات من جهاز الضحيه إلى جهاز المخترق ..

اذاً إلى اين سيتم ارسال البيانات !؟

.. صحيح . الى جهاز المخترق .. الـ [ip] الذي تم وضعه بداخل الباتش .. لكي يرسل المعلومات من جهاز الضحيه إلى الجهاز الذي يحمل ذلك الـ ip فقـط .

ومن البديهي ان المسؤول عن استقبال تلك البيانات وتحليللها .. هو برنامج الأختراق

مثال :

برنامج الأختراق : الأم

الباتش / Trojan : الأبن

ولكن يا Mr.Mo0oha أخبرتنا أن الـ ip address يتغير عندما يتم فصل المودم .. والعوده اليه مجدداً ؟! .. بهذا لن يتمكن المخترق من اختراق جهازي دائماً ؟! لأن الآي بي الموجود في الباتش ، اصبح مختلف عن الآي بي الخاص بالمخترق بعد انطفاء المودم !؟ كيف يتم ذلك !؟

حسناً .. هنالك طريقتين امام المخترق .. لكي لا يفقد ضحيته ..

1- ان يمتلك static-ip وهو ip لايمكن تغييره أي ثابت .. دائماً

2- ان يمتلك d-ip**** او ip إسمي . لنفصل هذه النقطه بعض الشيء .

تقوم عدة شركات اجنبيه .. بتوفير هذا النوع من الخدمات وهو الـ الآي بي الإسمي .. اذا صح التعبير بحيث يتم التعامل مع جهازك على اساس هذا الآي بي " الأسمي " .. ولا يتم التعامل معه مباشرة ..

كيف يتم ذلك !؟

من أهم الشركات التي تقدم هذه الخدمه هي no-ip

وموقعها الرسمي هو www.no-ip.com

وغيرها الكثير ..

يقوم الهكر بالتسجيل في الموقع .. وبعدها يتم انشاء host / مستضيف .. خاص به

س - لماذا يتم انشاء host / مستضيف ؟

ج - ليتم استقبل البيانات المرسله من أي جهه كانت إلى ذلك الـ host .. وليكن اسمه مثلاً

MrMo0oha.no-ip.com

.. اذاً / ماهو الآي بي الاسمي الآن !؟

صحيح .. MrMo0oha.no-ip.com

هذا هوَ

س. ولكن كيف سيتعامل المخترق مع الـ host الخاص به .. وينشىء إتصال بين جهازه وجهاز الشركه التي توفره له ذلك الـ host ؟

ج. تقدم الشركه برنامج .. يتم تركيبه على جهاز المخترق .. وبالتالي التواصل بينه وبين الـ host بحيث اذا تم وصول أي بيانات الى ذلك الهوست يتم ارسالها مباشرة إلى جهاز المخترق ..

أتمنى تكون وصلت الفكره :)

صوره للتوضيح ..



4 - تشفير الباتش .. وتجهيزه .

.. لابد ان الكثير يتساءل . أين برامج الحمايه ، من كل هذا ؟!

وأكثر المستخدمين يلجأون الى برامج الحمايه كأنها هي الحل الوحيد والمنقذ الأساسي ..

ومن أخبرك بذلك !؟

بالنسبة لي ، برنامج الحمايه لا يمثل سوى 60 % من الحماية .. وأقل من ذلك ايضاً .. المُتبقي يعتمد على فهمك لكيفية عملية الاختراق .. وماهية التروجانات / والأبواب الخلفيه .. التي قد يتم تثبيتها في جهازك بأراداتك .. ودون علمك بها .!

وَ لتجنب .. برامج الحمايه ؛ يقوم المخترق بتشفير [الباتش / back door / Trojan / حصان طرواده] .. لكي لا يتعرف عليه برنامج الحمايه ، ويتم معاملته كـ فرد من افراد عائلتك الالكترونيه [نظام تشغيلك / والبرامج المركبه عليه] .. ويتم السماح له بجميع العمليات التي يريدها] انشاء ملفات جديده في الريجستري / انشاء ملفات dll / ارسال واستقبال البيانات عبر بروتوكول tcp/ip] .. وذلك لأنه تم تشفير الباتش .. عن برنامج الحمايه !

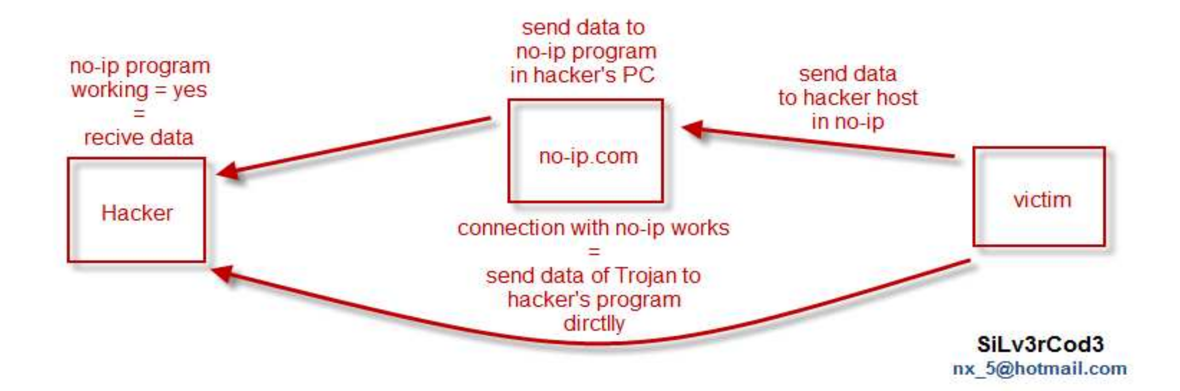
اذاً / برنامج الحمايه ليس كل شيء !

5 - الاتصال العكسي .. و وصول التبليغ .. وفوائدهما .

تحدثنا سابقاً عن طريقة الاتصال العكسي وهي بإستخدام احد المواقع التي تقدم هذه الخدمه .. مثل موقع www.no-ip.com وايضاً انشاء host لإستقبال البيانات المرسله إليه , ومن ثم ارسالها إلى جهاز الهكر ..

اذاً / جميع الاجهزه التي تم زرع الباتش فيها .. يتم ارسال بياناتها الى هذا الهوست .. ومن ثَم تصل هذه المعلومات الى جهاز الهكَر ..

صوره للتوضيح :



6 - انشاء الاتصال بين جهاز المخترق وجهاز الضحيه / طرق ارسال الباتش .

جميع الطرق تؤدي إلى روما !

تختلف طرق ارسال الباتش من هكر إلى آخر .. حسب معرفته وخبرته في هذا الأمر .. فبعضهم يستغل عدم علم ضحيته بـ امتدادت الملفات ..

أي لا يستطيع التمييز بين صيغة jpg و exe !!!

وهذهِ هي النوعيه المفضله لدى الهكرز ، التي ليس لها علم بشيء ..

ولكن ايضاً قد يواجه الهكر .. ضحايا يعلمون بأمور الكمبيوتر ، ويعرفون مداخله ومخارجه .. ولكنهم لا يعلمون الا القليل عن كيفية الاختراق ، و كيف يتم ..

لذلك .. يعتمد فقط على علمه المحدود .. أي انَ اذا ارسل الهكر لهُ ملف بأمتداد Exe يبدأ بالشك ويعتقد ان هذا باتش !

وقد يرسل له الهكر ملف بأمتداد Jpg فـ يطمئن ، ويلغي أي شك لديه أن هذا الملف قد يكون باتش !!

لكن ، الآن في عام 2010 .. أجزم ان جميع صيغ الملفات قد تصبح باتشات ..

سواءً كانت ملفات مكتبيه .doc , .pdf .. etc

او ملفات اغاني mp3 , rmv , wmv ... etc

او ملفات صور jpg , jpeg , gif ,bmp ... etc

جميعها ، قد تكون اساساً ملفات [Trojan / حصان طروآده / patch] .

و تتعدد طرق ارسال الباتش وهي كثيره سأكتفي بذكر المُهم منها :

1 - عن طريق المحادثات [ماسنجر / ياهو / سكايبي]

2 - روابط ملغومه :

ماذا يعني رابط ملغوم ! ..

يعني ان الهكر .. قام برفع صفحه من انشاءه ، او قام بالتعديل عليها ..

لكن .. كيف يتم ارسال الباتش الى جهازي عندما ادخل هذه الصفحه ؟

مثلاً الصفحه [الرابط الملغوم]

www.SiLv3Rcod3.com/about.htm

www.SiLv3Rcod3.com/Me.jpg

بأي صيغة كان امتداد الملف .. المهم في الرابط الملغوم هوَ ..

عندما يقوم الهكر بالتعديل على هذه الصفحه .. ويرفعها مره أخرى .. يقوم بأضافه ثغرة من ثغرات المتصفح .. والمتصفح الذي يستخدمه أغلب المستخدمين دائماً هو IE لذلك يتم وضع ثغرة مناسبه ، تسمح هذه الثغره بتنزيل ملف الباتش في مجلد الـ Startup / بدء التشغيل .. لكي يتم تشغيل الباتش .. بعد عمل أول رستارت للجهاز .. وليس بالضروره فقط ملف Startup ولكن يمكن استخدام الثغره عدة استخدامات ... وهي ليست موضوع حديثنا الان !

3 - دمج الباتش بـ برامج أخرى ونشرها في المنتديات !

لذلك يجب على الجميع الحذر من الملفات التي يتم تحميلها من الانترنت .. والتأكد انها من مصادر موثوقه ..

.. والكثير من الطرق المختلفه والمتنوعه والتي تؤدي في نهاية المطاف إلى اختراق جهازك ..

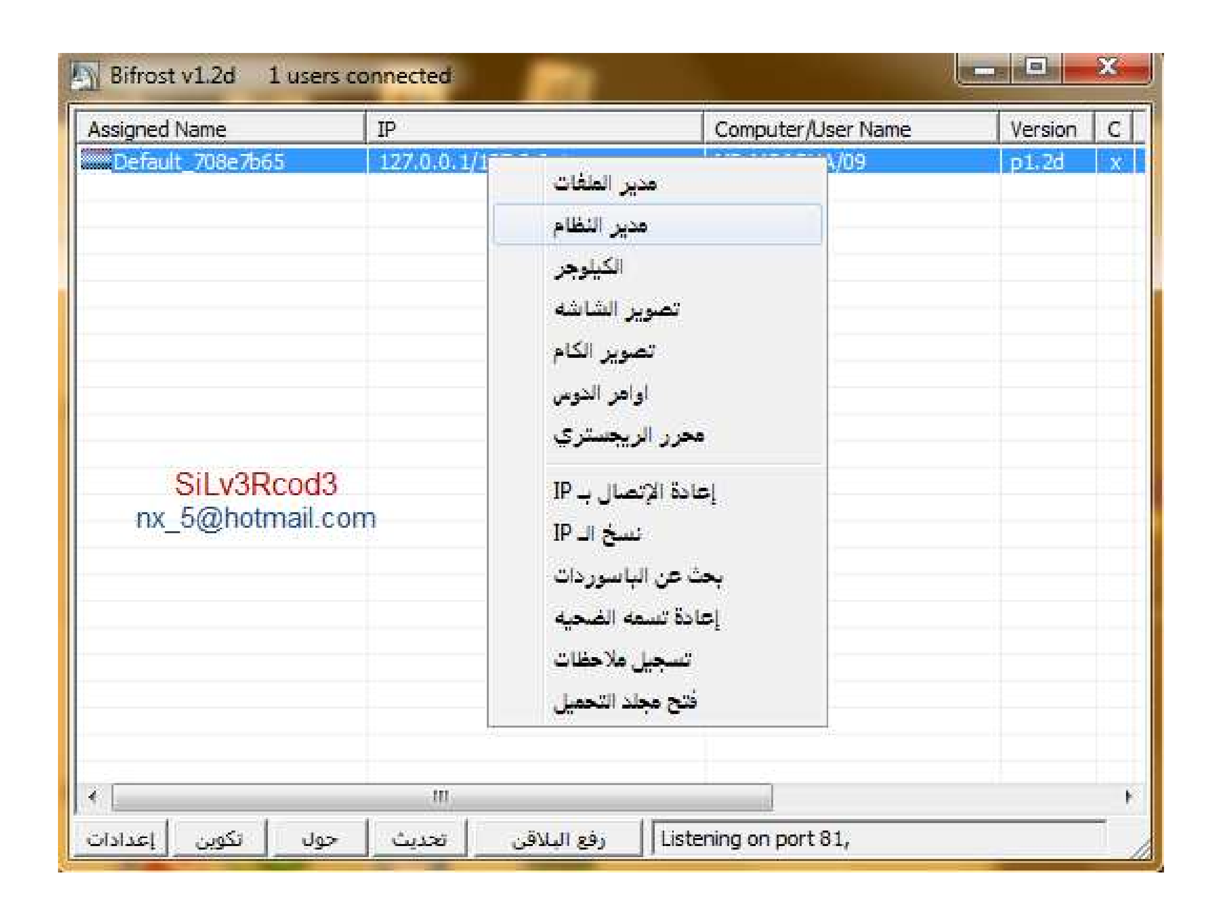
7 - استخدام برنامج الأختراق .. بعد الاتصال .

اذاً ، تم ارسال الباتش .. وتشغيله في جهاز الضحيه .. وتم استقبال البيانات المرسله من الباتش إلى برنامج الأختراق في جهاز الهكر ..

بهذا ، تم الأختراق 100%

لكن ماذا عن خصائص ، برنامج الإختراق .. وليكن برنامج biforst مثلاً !؟

صوره للتوضيح / خصائص برنامج biforst



جميع الخيآرات متآآحه .. وطبعاً تختلف خصائص كل برنامج عن الآخر ..

8 - ما الذي قد يحصل لجهازي عندما اصبح ضحية لمخترق ؟

هل ترى كل تلك الخصائص التي يوفرها برنامج الأختراق لـ الهكر !! ..

يستطيع الهكر تنفيذها كاملة ..

ايضاً بالاضافه الى جميع تلك الخصائص .. يستطيع الهكر رفع فيروسات .. وتشغيلها على جهازك ..
تؤدي تلك الفيروسات الى ضرب قطع مهمه في الجهاز منها الماذربورد / والهارد / و المعالج .. Etc

أي انكَ اصبحت أنت وجهازك " لُعبه " لدى الهكر ... يتحكم بها كيفما شاء ..

9 - هل يمكنني تفادي ذلك ؟

بالطبع يمكنك تفادي ذلك ..

يُنصح في حالة الشك بوجود اختراق .. بفصل النت نهائياً عن الجهاز .. ومن ثَمَ معاينة مواضع الخلل التي أصيبت ..

. لا يسعني الوقت لذكر طرق تفادي الاختراق في الوقت الحالي ..

ولكن ..

سيتم شرحها .. ضمن سلسلة دروس حماية الجهاز من الأختراق .. إن شاء الله

إلى هنا ، ينتهي موضوع " ميكانيكية أختراق الأجهزه " .. بجزئيه الأول والثاني ..

أتمنى ان اكون قد وفقت في شرح هذا الموضوع ..

ان اصبت فـ توفيق من الله ، وان اخطأت فـ من نفسي والشيطان ..

لا اسألكم سوى الدعاء لي ولوآلدي بالرحمه والمغفره ..

والسلام عليكم ورحمة الله وبركـــاته

* ملاحظـات .. Notes

================================

- الأيميل المذكور على الصور ، ليس للمساعده .. فقط لحفظ الحقوق .. !

Author :

Mohammed Nasser Al-Mawri